

***ACP***





## Hannes Lagler-Gruener

Cloud Solutions Architect, ACP

P-CSA, Azure MCSE, AWS Cloud Practitioner

**Blog** <http://cloudblogger.at>

**Sozial** <https://www.linkedin.com/in/hannesl1>

# Ziel dieses Workshops

- Was ist Azure?
- Wie kauft man Azure bzw. welche Vertragsarten gibt es?
- Ein Überblick über die Azure Services
- Sicherheit in der Azure Cloud
- Umgesetzte Use-Cases für die Cloud
- Netzwerk und Anbindungsmöglichkeiten an die Azure Cloud
- Kostenübersicht und Forecast-Möglichkeiten

# Agenda

09:00 – 10:30

➤ Start

10:30 – 10:45

➤ Pause

12:00

➤ Mittagessen

13:00

➤ Start Nachmittag

14:30

➤ Kaffee

16:00

➤ Finale – Feedback Runde

➤ Fragen, Fragen, Fragen

**The future is already here it's just  
not very evenly distributed.**

William Gibson



Gold Cloud Productivity  
Gold Cloud Platform  
Gold Datacenter  
Gold Devices and Deployment  
Gold Enterprise Mobility Management



Microsoft Country  
Partner of the Year 2017

Größter **CSP Direct**  
Partner in Österreich

>47

Consultants österreichweit,  
die bereits Cloud-Projekte  
umgesetzt haben

>95.151

betreute Mailboxen  
in der Cloud

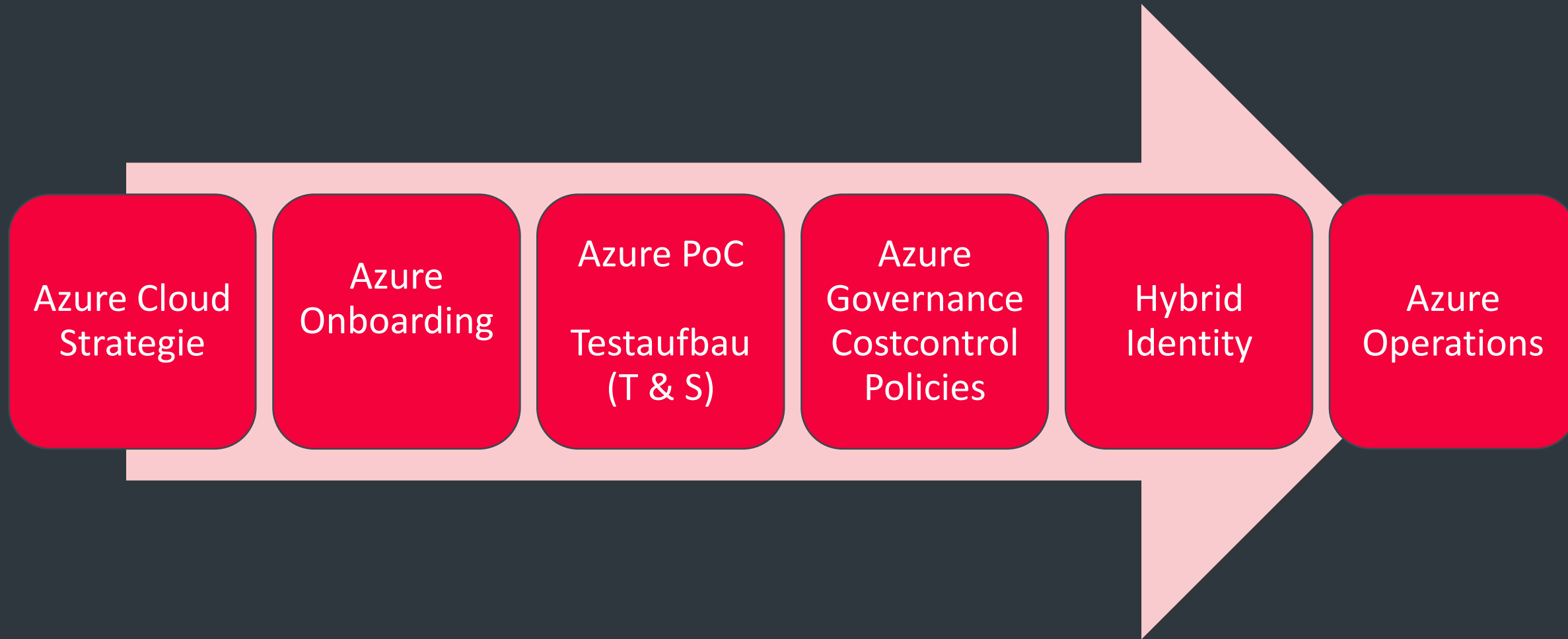
>990

Office 365  
Kunden

>1,5 Mio.

Euro Azure Umsatz  
im Jahr

## ACP public cloud offerings



# Was ist Azure?



# Ziel dieses Workshops

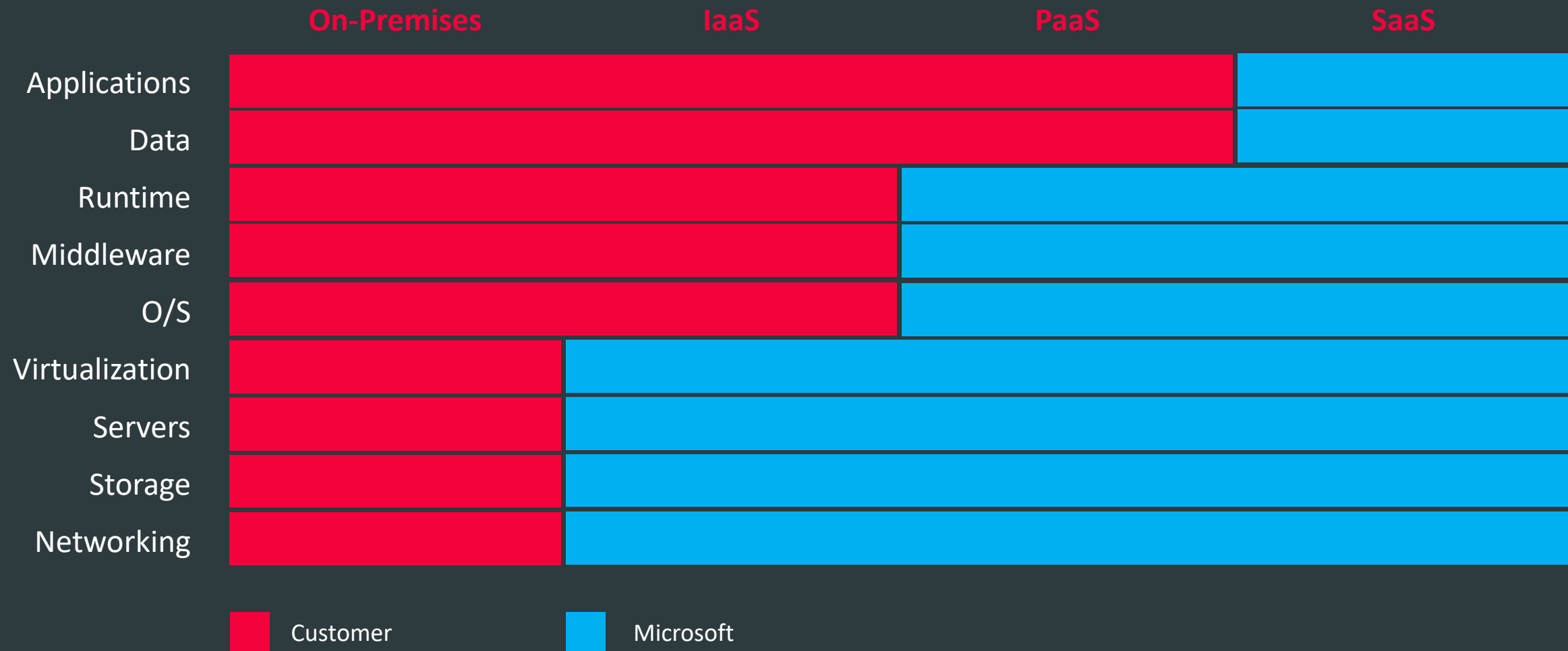
- Globales Rechenzentrum in 54 Regionen (Stand 04.2019)
- Rechenzentren sind „managed by Microsoft“
- Hoch skalierbare Cloud Computing Plattform
- Hohe Verfügbarkeit der Services
- Hoher Automatisierungslevel
- Hohe Kostentransparenz
- Verteilte Aufgabenteilung (IaaS, PaaS, SaaS,...)
- Hybrid Cloud Anbieter
- Herstellerunabhängig
- Schnell und flexibel
- ...

**54** regions worldwide **140** available in 140 countries



- Available region
- Announced region
- ◆ Availability Zones

\* Two Azure Government Secret region locations undisclosed





**Was ist Azure?**  
Azure ist offen

## Azure is an open cloud



# Wie kaufe ich Azure



## Azure kaufen

- Gratis Testversion (1x EUR 170)
- MSDN Abo (Monatlich max. EUR 170)
- Direkt bei Microsoft
- Enterprise Agreement
- Partner (CSP)



## Azure kaufen Modelle und Lizenzen

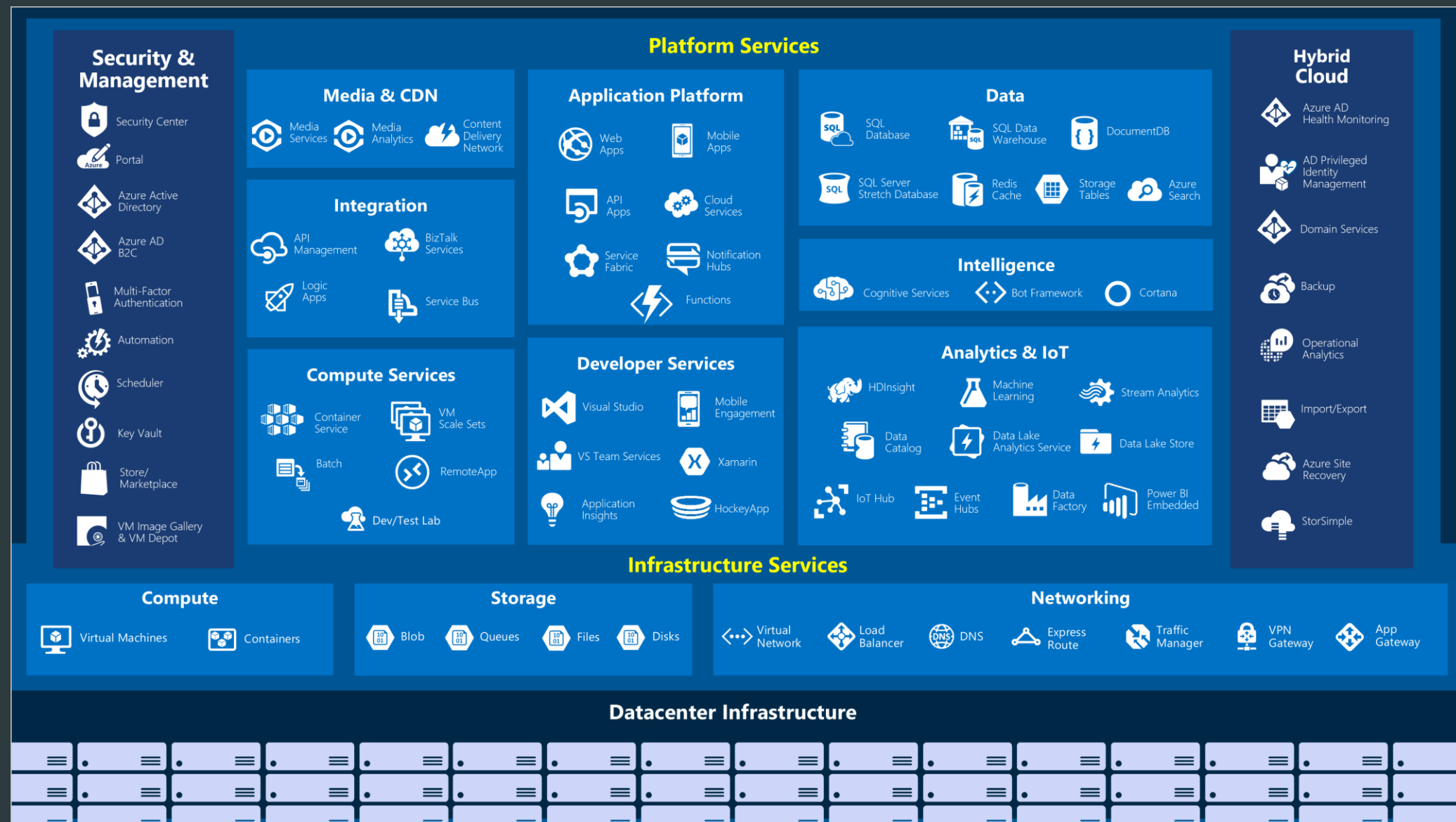
- Pay as you go (per Hour, GB, Minutes, Traffic,...)
- Upfront Commit
- Reserved Instances
- Azure Hub Licensing
- Byol (Bring your own license)
- ...

# Überblick Azure Services





# Azure Services





# Azure Services Infrastructure

## Compute



Virtual Machines



Containers

## Storage



Blob



Queues



Files



Disks

## Networking



Virtual  
Network



Load  
Balancer



DNS



Express  
Route



Traffic  
Manager



VPN  
Gateway



App  
Gateway



## Azure Services Security & Management

### Security & Management



Security Center



Portal



Azure Active  
Directory



Azure AD  
B2C



Multi-Factor  
Authentication



Automation



Scheduler



Key Vault



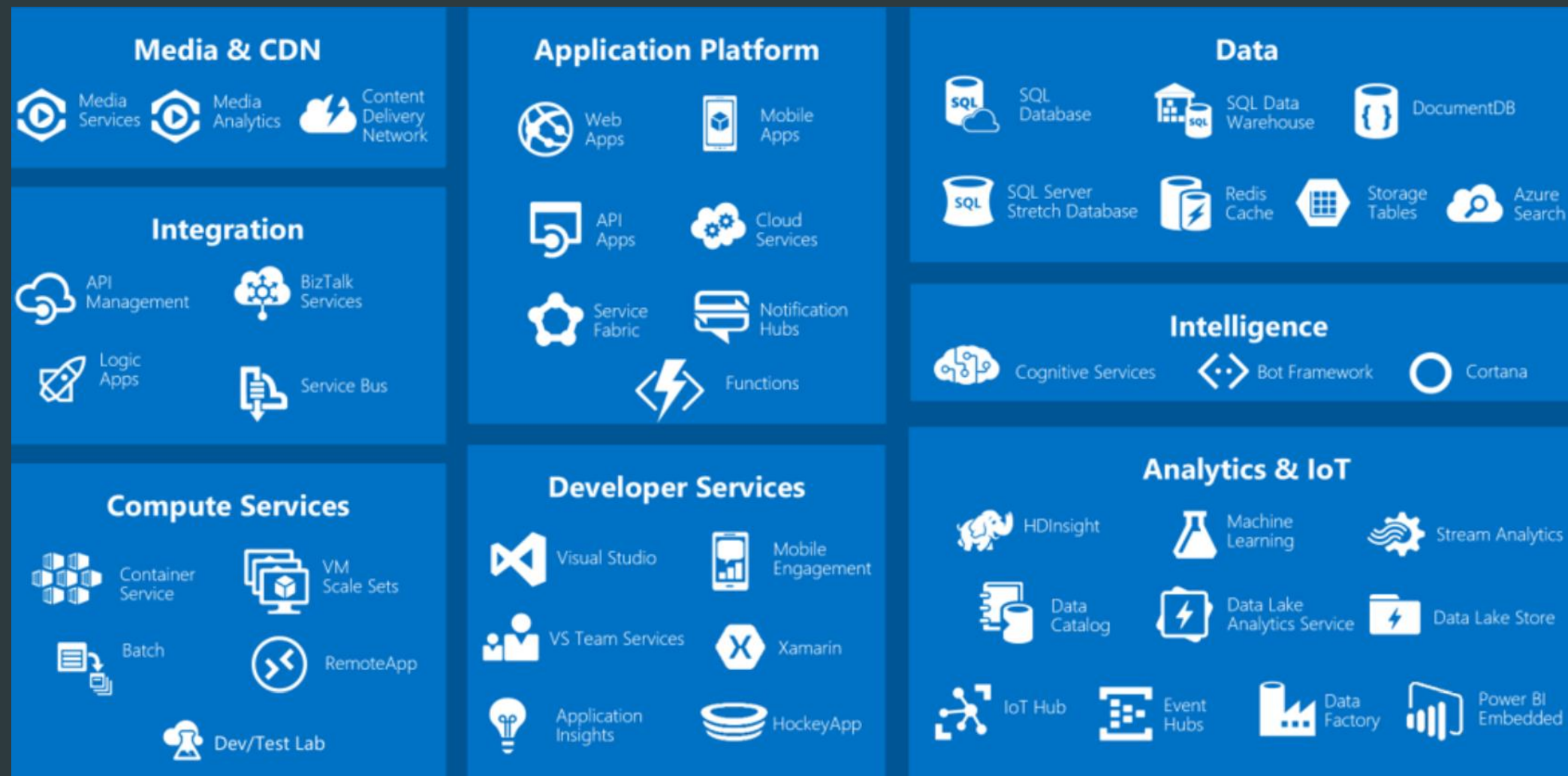
Store/  
Marketplace



VM Image Gallery  
& VM Depot



# Azure Services Platform Services





# Azure Services Hybrid Operations

## Hybrid Cloud



Azure AD  
Health Monitoring



AD Privileged  
Identity  
Management



Domain Services



Backup



Operational  
Analytics



Import/Export



Azure Site  
Recovery



StorSimple

# Azure Marketplace

**Microsoft Azure**

Search resources, services, and docs

stefan.denninger@ac...  
ACP OST INT

Create a resource

Home

Dashboard

All services

FAVORITES

Subscriptions

Resource groups

All resources

App Services

Azure Active Directory

Automation Accounts

Azure Cosmos DB

SQL databases

Virtual machines

Load balancers

Storage accounts

Virtual networks

Monitor

Advisor

Security Center

Reservations

Cost Management + Billing

Dashboard > New > Marketplace

Marketplace

Categories

Get Started

Compute

Networking

Storage

Web

Mobile

Containers

Databases

Analytics

AI + Machine Learning

Internet of Things

Mixed Reality

Integration

Security

Identity

Developer Tools

Management Tools

Software as a Service (SaaS)

Blockchain

Compute

Ubuntu Server 18.04 LTS

Canonical

Ubuntu Server delivers the best value scale-out performance available.

Red Hat Enterprise Linux 7

Red Hat

Red Hat Enterprise Linux 7 is the world's leading enterprise Linux platform built to meet the needs of

Windows Server

Microsoft

Microsoft Windows Server Virtual Machine Images

SQL Server 2017 on Windows Server 2016

Microsoft

SQL Server 2017 images on Windows Server 2016

Virtual machine scale set

Microsoft

Deploy multiple instances of a single image.

Cloudera on Azure

Cloudera

Cloudera Enterprise Data Hub

See More

Networking

Virtual Network

Microsoft

Create a logically isolated section in Microsoft Azure and securely connect it outward.

Load Balancer

Microsoft

A load balancer that distributes incoming traffic among backend virtual machine instances.

Application Gateway

Microsoft

Scalable layer-7 load balancer offering various traffic routing rules and SSL termination for backend

Firewall

Microsoft

Azure Firewall is a managed cloud-based network security service that protects your Azure Virtual Network

Front Door

Microsoft

Azure Front Door Service is Microsoft's highly available and scalable web application

Virtual WAN

Microsoft

Azure Virtual WAN is a networking service that provides optimized and automated branch-to-branch

See More

Storage

Azure Data Box

Microsoft

Migrate your data to cloud with ease.

Data Lake Storage Gen1

Microsoft

Hyper-scale repository for big data analytic workloads

Nasuni Cloud File Services (NMC)

Nasuni

Nasuni Cloud File Services (NMC)

Data Box Edge / Data Box Gateway

Microsoft

Manage Data Box Edge/Gateway appliance.

Veritas NetBackup™

VERITAS

Instantly access Enterprise Data Protection in Microsoft Azure and set it up your way.

Azure AD Privileged Identity Management

Microsoft

Azure AD Privileged Identity Management (PIM) manages privileged access rights of your

See More

# Azure Stack Marketplace

Microsoft Azure Stack

Search resources

stefan.denninger@ac...  
ACP OST INT

Home > New > Marketplace > Everything

Create a resource

All services

FAVORITES

Dashboard

All resources

Resource groups

Virtual machines

Subscriptions

Recent

Images

Storage accounts

Monitor

Metrics

Virtual networks

DNS zones

Local network gateways

Marketplace

Everything

Offers + Plans

Compute

Data + Storage

Networking

Custom

Security + Identity

Data + Analytics

Web + Mobile

Developer Services

Management

Popular

Key Vault  
[Learn more](#)

Storage account - blob, file, table, queue  
[Quickstart tutorial](#)

Template deployment  
[Learn more](#)

Most recently created

Connection  
[Learn more](#)

Windows Server 2016 Datacenter - with Containers - BYOL use only  
[Learn more](#)

Filter

Search Everything

Compute

Ubuntu Server 16.04 LTS  
Canonical

Availability Set  
Microsoft

Kubernetes Cluster (preview)  
Microsoft

Free License: SQL Server 2016 SP2  
Microsoft

Windows Server 2012 R2  
Microsoft

Windows Server 2016 Datacenter -  
Microsoft

Networking

Connection  
Microsoft

DNS zone  
Microsoft

Load Balancer  
Microsoft

Local network gateway  
Microsoft

Network interface  
Microsoft

Network security group  
Microsoft

Security + Identity

Key Vault  
Microsoft

Barracuda CloudGen Firewall  
Barracuda Network...

Commvault Trial  
Commvault

F5 BIG-IP VE - ALL (BYOL, 1 Boot  
F5 Networks

FortiGate NGFW - Single VM  
Fortinet

BYOL Load Balancer, ADC &  
KEMP Technologies ...

Offers + Plans



# Demo

Azure Portal

Azure Marketplace

Azure IaaS

Azure PaaS (WebApp, Storage)



# Sicherheit in der Azure Cloud



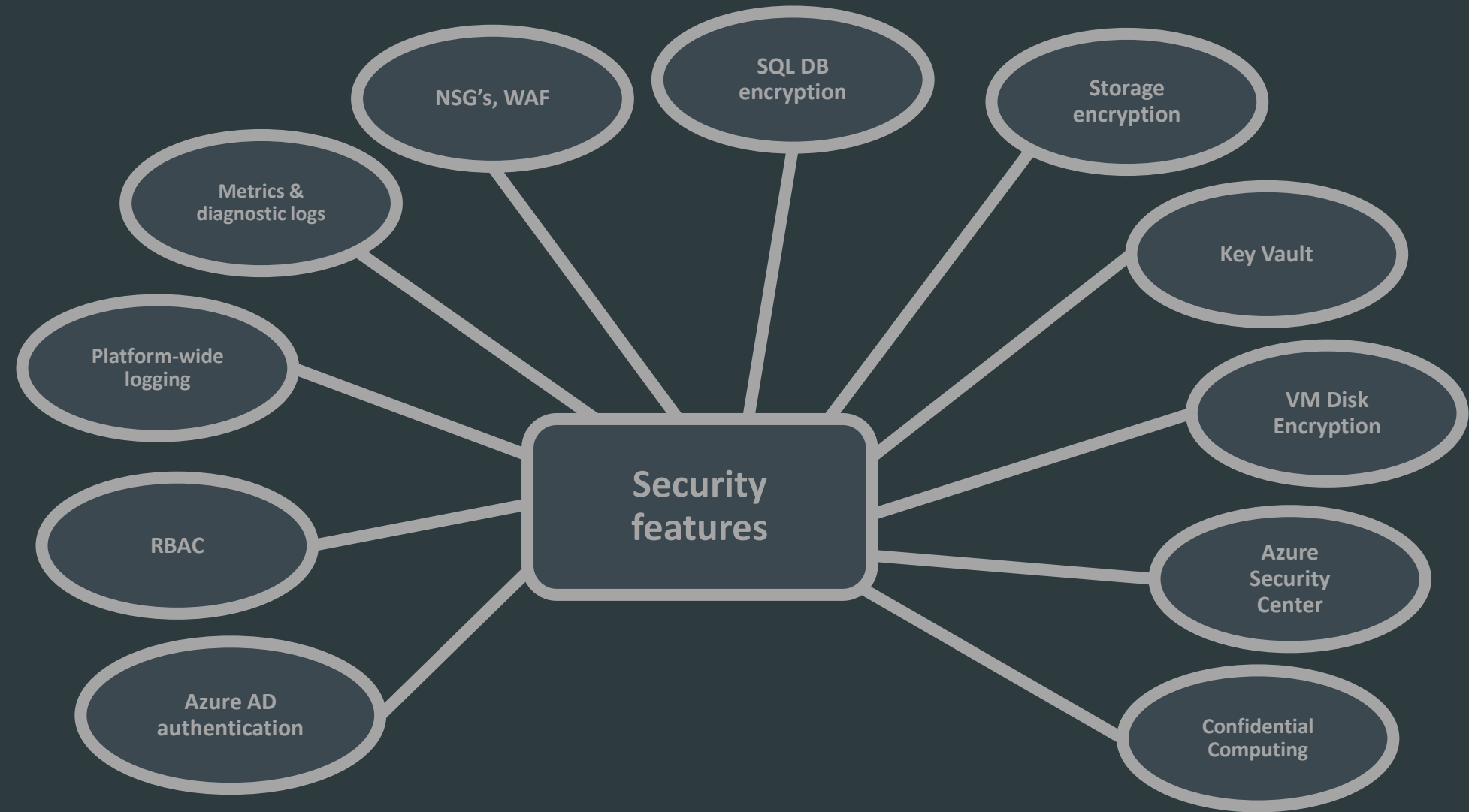
# Sicherheit in Azure

GLOBAL	 ISO 27001	 ISO 27018	 ISO 27017	 ISO 22301	 ISO 9001	 SOC 1 Type 2	 SOC 2 Type 2	 SOC 3	 CSA STAR Self-Assessment	 CSA STAR Certification	 CSA STAR Attestation							
US GOV	 Moderate JAB P-ATO	 High JAB P-ATO	 DoD DISA SRG Level 2	 DoD DISA SRG Level 4	 DoD DISA SRG Level 5	 SP 800-171	 FIPS 140-2	 Section 508 VPAT	 ITAR	 CJIS	 IRS 1075							
INDUSTRY	 PCI DSS Level 1	 CDSA	 MPAA	 FACT UK	 Shared Assessments	 FISC Japan	 HIPAA / HITECH Act	 HITRUST	 GxP 21 CFR Part 11	 MARS-E	 IG Toolkit UK	 FERPA	 GLBA	 FFIEC				
REGIONAL	 Argentina PDPA	 EU Model Clauses	 UK G-Cloud	 China DJCP	 China GB 18030	 China TRUCS	 Singapore MTCs	 Australia IRAP/CCSL	 New Zealand GCIO	 Japan My Number Act	 ENISA IAF	 Japan CS Mark Gold	 Spain ENS	 Spain DPA	 India MeitY	 Canada Privacy Laws	 Privacy Shield	 Germany IT Grundschutz workbook

Quelle: <https://servicetrust.microsoft.com/Documents/ComplianceReports>



## Sicherheit in Azure Continue





## Sicherheit in Azure Azure AD Continue

# Service seitens ACP

- Segregation of duty
- Best practice seitens Microsoft
- Best practice seitens ACP
- Auswertung anhand definierter Bewertungsmethodik
- Umsetzung der Auswertung in Abstimmung

### 1.2. BEWERTUNGSMETHODIK

Als Ergebnis wird ein Gesamtrisikofaktor für ein Finding in den Kategorien „Niedrig“, „Mittel“, „Hoch“ und „Kritisch“ definiert.

Kritische Findings erfordern sofortige Aufmerksamkeit, da sie eine Verwundbarkeit darstellen, die unmittelbar ausgenutzt werden und potentiell zu einem hohen Schaden führen kann.

Mit „Hoch“ bewertete Findings sollten dringend bezüglich ihrer Auswirkung auf die Geschäftsprozesse bewertet werden, um entsprechende Maßnahmen ableiten zu können.

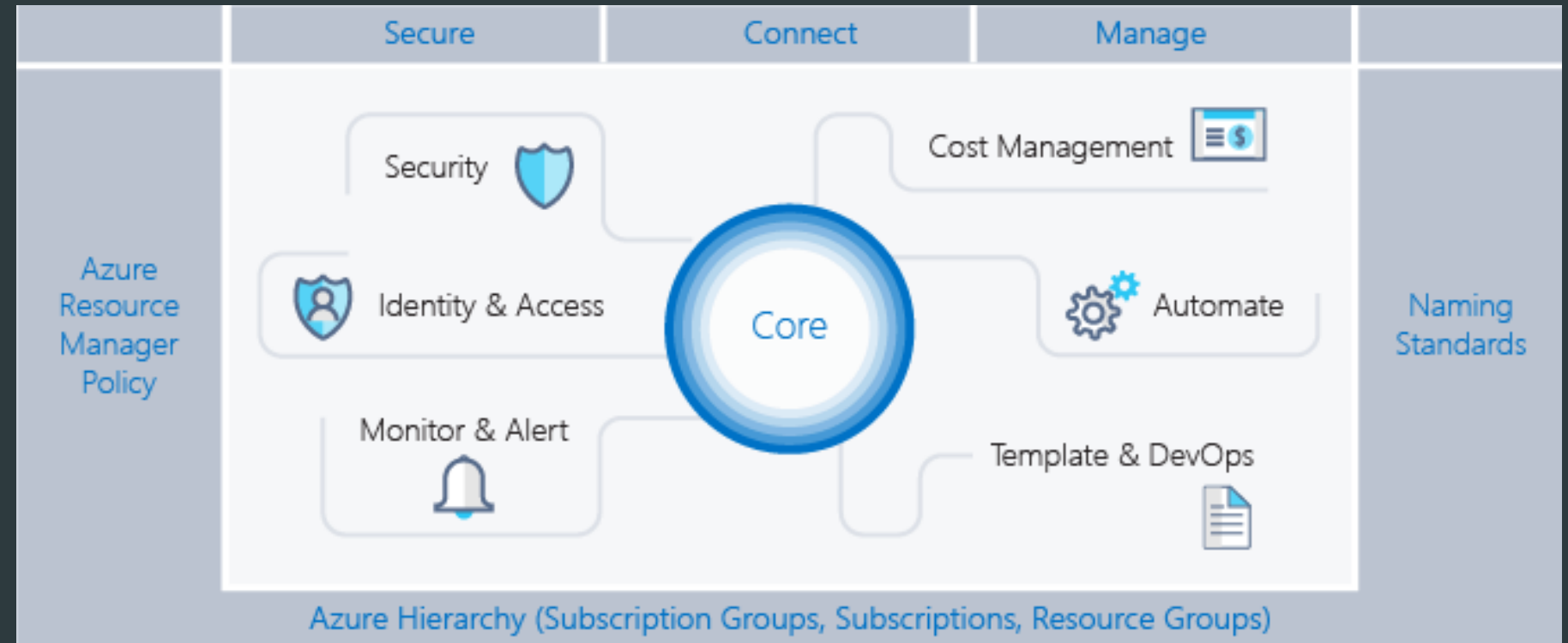
Findings, die mit „Mittel“ bewertet sind, sollten im Rahmen des Risikomanagements des Unternehmens bewertet werden, um Maßnahmen zur Behebung der Schwachstelle oder zur Reduktion des Risikos abzuleiten.

Findings mit „Niedrig“-Bewertung sollten ebenso in das Risikomanagement einfließen, erfordern aber keine zeitnahe Reaktion.

Auswirkung	sehr hoch	M	H	K	K
	hoch	M	M	H	K
	mittel	N	M	M	H
	gering	N	N	M	M
		gering	mittel	hoch	sehr hoch
		Verwundbarkeit			



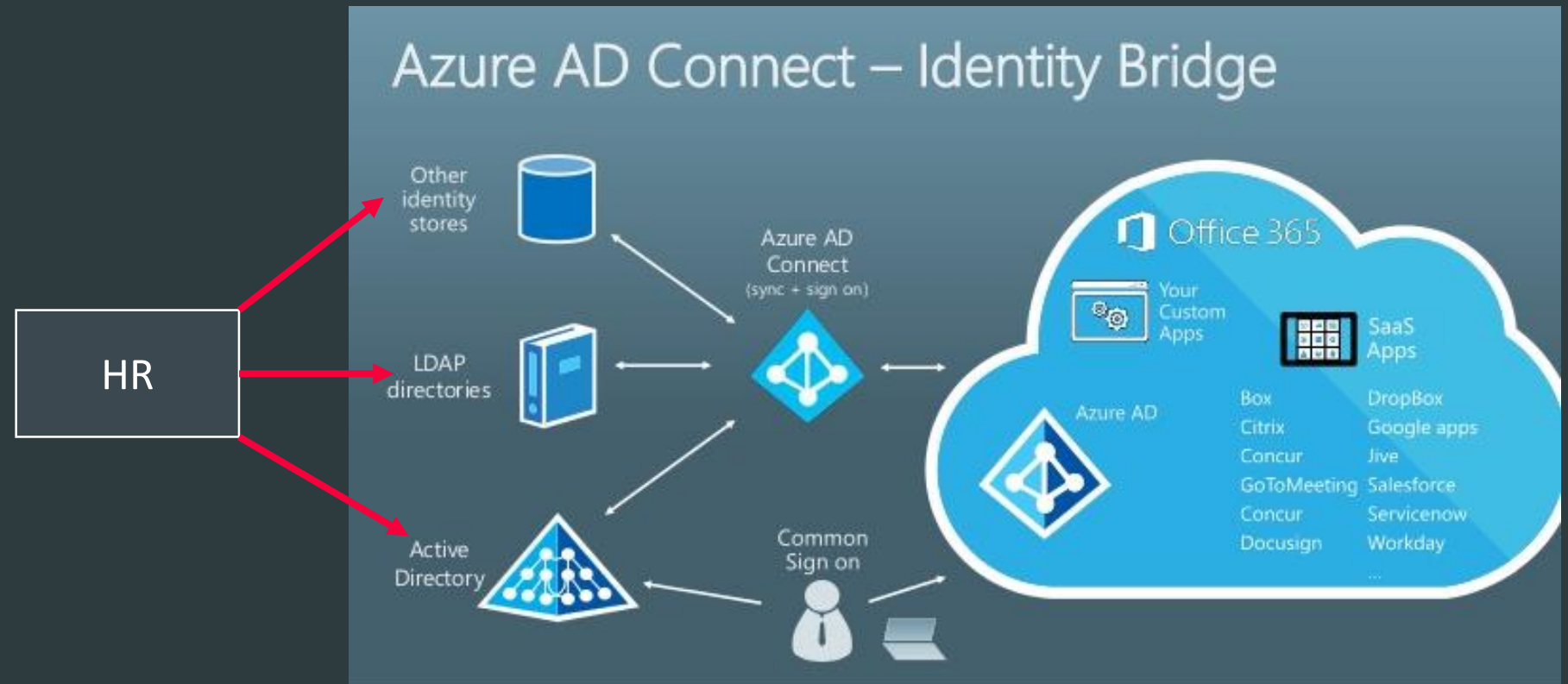
## Sicherheit in Azure Governance



- Azure Management Groups
- Azure BluePrint



## Sicherheit in Azure Azure AD





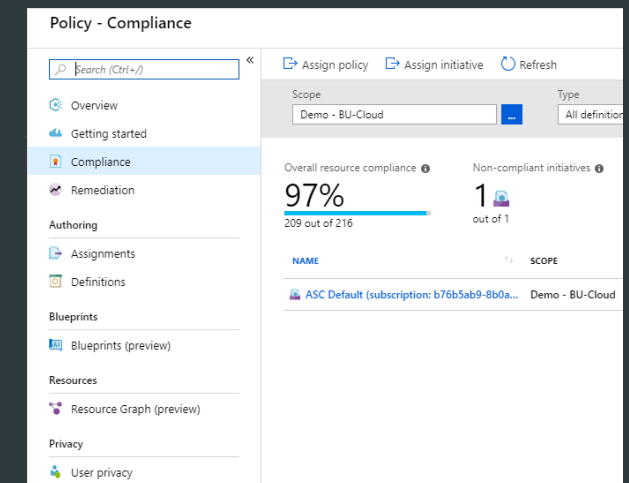
## Sicherheit in Azure Ressource Policies

### Zwei Säulen Azure Policy und Azure-Initiativen

- Azure-Policy
- Richtlinien in ihren Unternehmen definieren
- Geografische Compliance/Datenhoheit
- Vermeidung öffentlich verfügbarer Server
- Überwachen und Einschränken

### Azure-Initiativen

- Sammlung aus Azure-Policies





## Sicherheit in Azure Naming Standards

- Ein sehr wichtiger Task
- Ermöglicht eine einfachere Identifizierung von Ressourcen
- Einfachere Verteilung von Daten in Dashboards und Abrechnung
- Einfacher Standardisierung bei Automatisierung
- Namen sind nachträglich schwer zu ändern!

Beispiel eines Namens Schemas:

```
<Company> <Department (optional)> <Product Line (optional)> <Environment>
```

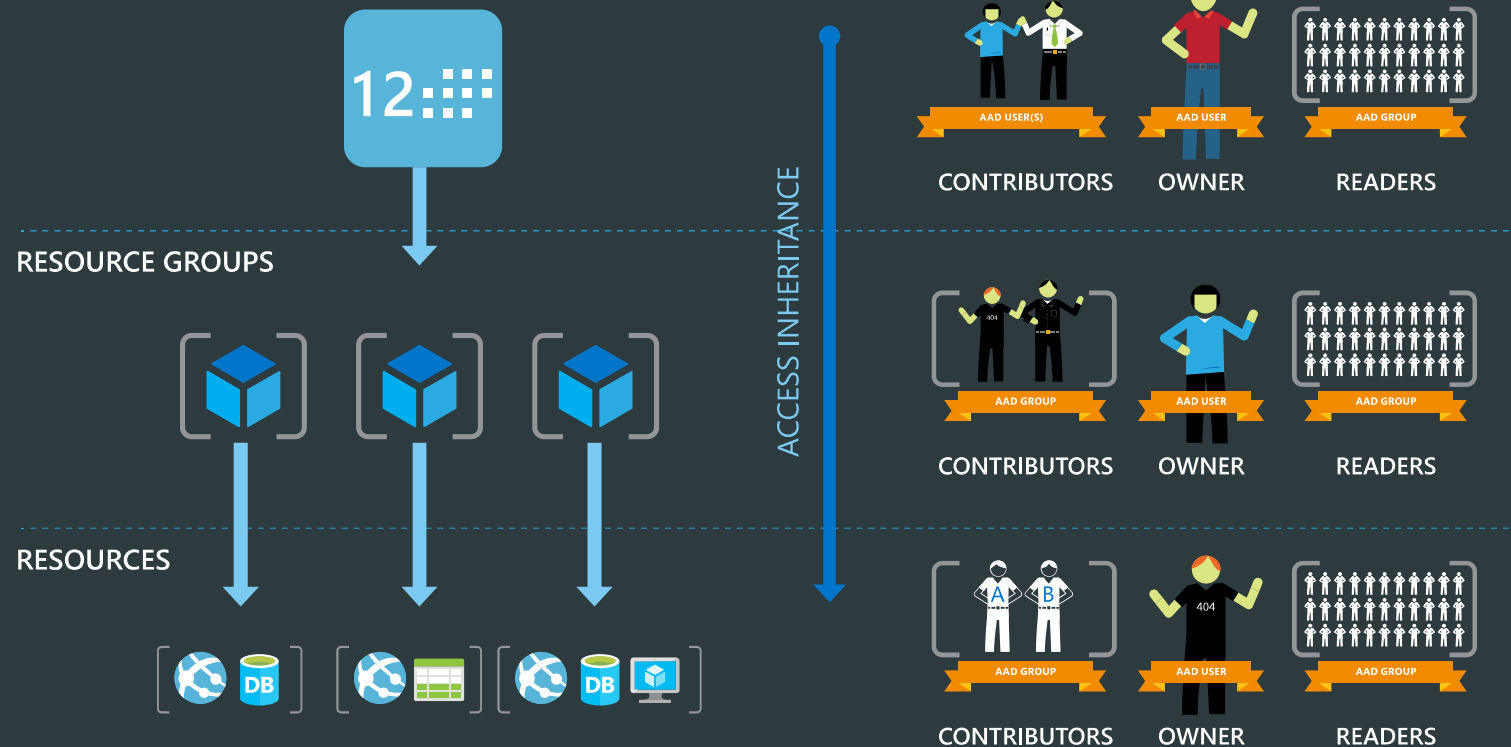




## Sicherheit in Azure RBAC

- > Beschreibt die Berechtigungen (z. B. Leseberechtigung)
- > Kann mehrfach gebunden werden
- > Berechtigung wird einem/r User/Gruppe und mit einem Scope (Bsp. Ressource Group) zugewiesen
- > Erlaubt eine Vererbung

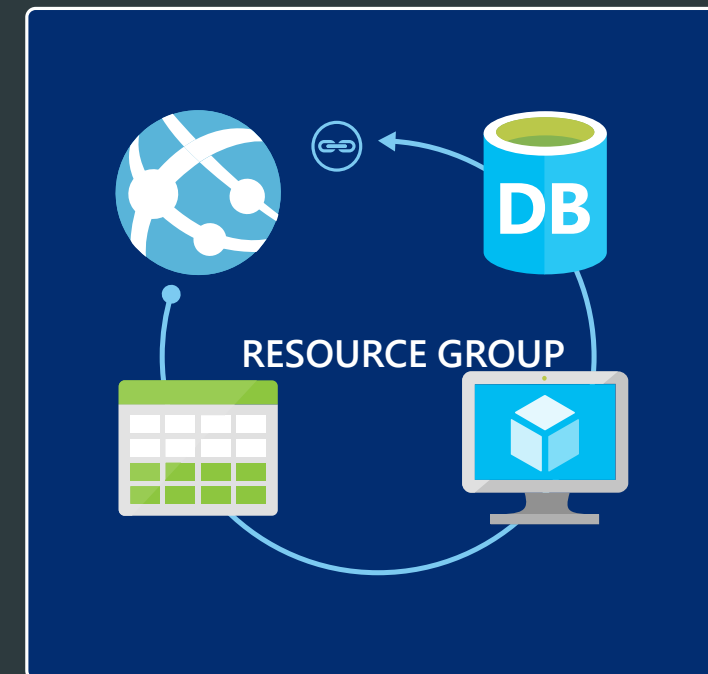
SUBSCRIPTION





## Sicherheit in Azure Resource Groups

- Zusammenfassung von Ressourcen in einen Container
- Enthaltene Ressourcen sollten von gleichem Lebenszyklus sein
- Jede Ressource darf nur an eine Ressource Group gebunden sein
- Ressourcegruppen sind nicht an Regionen gebunden
- Keine Verschachtlung unterstützt
- Nur Subscription Owners können Ressourcegruppen erstellen



Tags sind ein Metadata Speicher






**Beispiel:**

- Environment, e.g. dev/test/prod
- Role, e.g. web/cache/db
- Application name, e.g. CRM
- Department, e.g. finance/retail/legal
- Responsible party, e.g. Bob



## Sicherheit in Azure Ressource Tags

**Tags sind u.a. wichtig für 3rd party management solutions (CheckPoint NVA,..)**

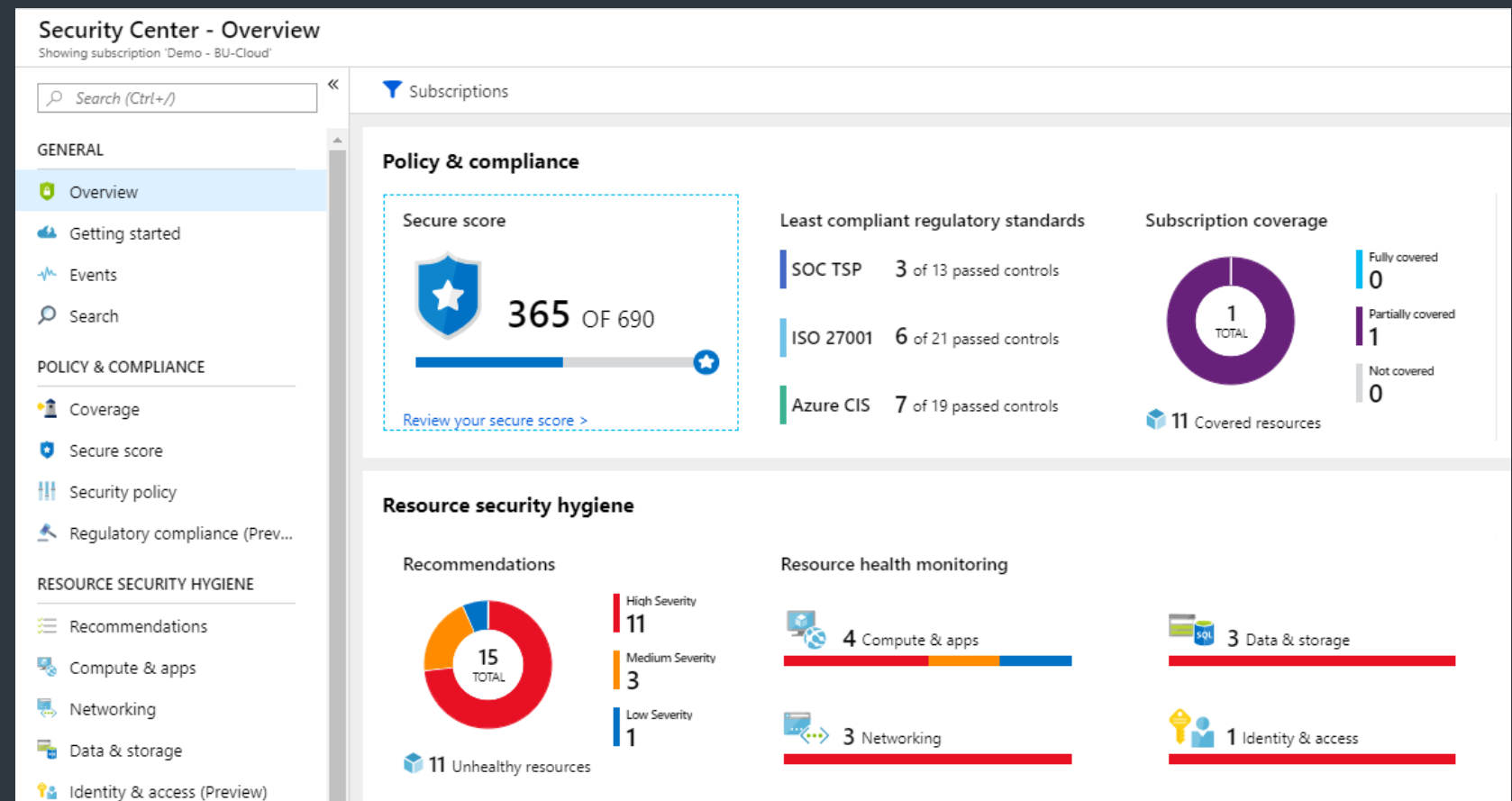
Resource groups			
Microsoft			
+ Add Columns Refresh			
Subscriptions: 1 of 3 selected – Don't see a subscription? <a href="#">Switch directories</a>			
Filter items... Internal Policy Test Subscription			
NAME	COSTCENTER (TAG)	ENVIRONMENT (TAG)	APPLICATION NAME (TAG)
 ContosoApp001	98052	Production	Contoso ERP App ...
 ContosoApp002	98052	Testing	Contoso ERP App ...
 CRMProd	98074	Production	Contoso CRM Online ...
 CRMTesting	98074	Testing	Contoso CRM Online ...
 demoapp	98074	Testing	Loan processing app demo ...

# Azure Automation

- Zentrale Automatisierungsebene
- Ziel sollte sein IaC (Infrastructure as Code) oder EasC (Enterprise as Code)
- Automatisierung mittels Powershell und ARM Templates (JSON Format) durchgängig möglich
- Hybrid Szenarien möglich (Hybrid Worker)
- Serverless
- Pay-as-you-Go
- DSC Pull Server eingebaut
- Update Management kostenfrei dabei

# Azure Security Center

- Zentrales Monitoring der Azure Umgebung
- Beinhaltet Best Practice und Verbesserungsvorschläge
- Hybrid Szenarien möglich
- Es gibt eine Free und eine Pay-as-you-Go Variante



# Demo

- Azure Policies
- Azure RBAC
- Ressource Groups
- Tags
- Locks
- Automation
- Security Center
- Azure Management Groups

# Use-Cases für die Cloud

# Use-Cases für die Cloud

- SAP on Azure
- IoT Szenarien on Azure oder Hybrid (Azure Stack)
- Backup2Cloud
- Azure Webapplication global hosten
- Azure SQL, SQL Managed Instance
- Azure AI Szenarien
- uvm.



# Netzwerk und Anbindung



## Azure Netzwerk

- Vollwertiger Layer3 Netzwerk und nur teilweise Layer2
- DHCP, kein Broadcast / Multicast!
- IP Adresse Bereich / Subnet
- VMs können nur in Subnetze deployed werden
- PaaS Integration möglich

**Name:** VNet1

**Address space:**

- 10.57.0.0/16
- 10.66.0.0/24

**Subnet1**  
10.57.1.0/24

VM1

VM3

VM2

**Subnet2**  
10.66.0.0/24

VM4

VM5

VM6

VM7



## Azure Netzwerk NSGs

### NSGs key facts

- 5-Tupel-ACLs
- Quell-IP, Ziel-IP, Quellport, Zielport, Protokoll (TCP, UDP, beliebig)
- Aktionen: erlauben oder ablehnen
- Wegbeschreibung: Inbound, Outbound
- Priorität: 100-4096 (niedrigerer Wert = höhere Priorität)

### Stateful

- Rückweg muss nicht konfiguriert werden!

## Kann auf NICs und Subnetze (ARM) angewendet werden

### Eingehende Verbindungen

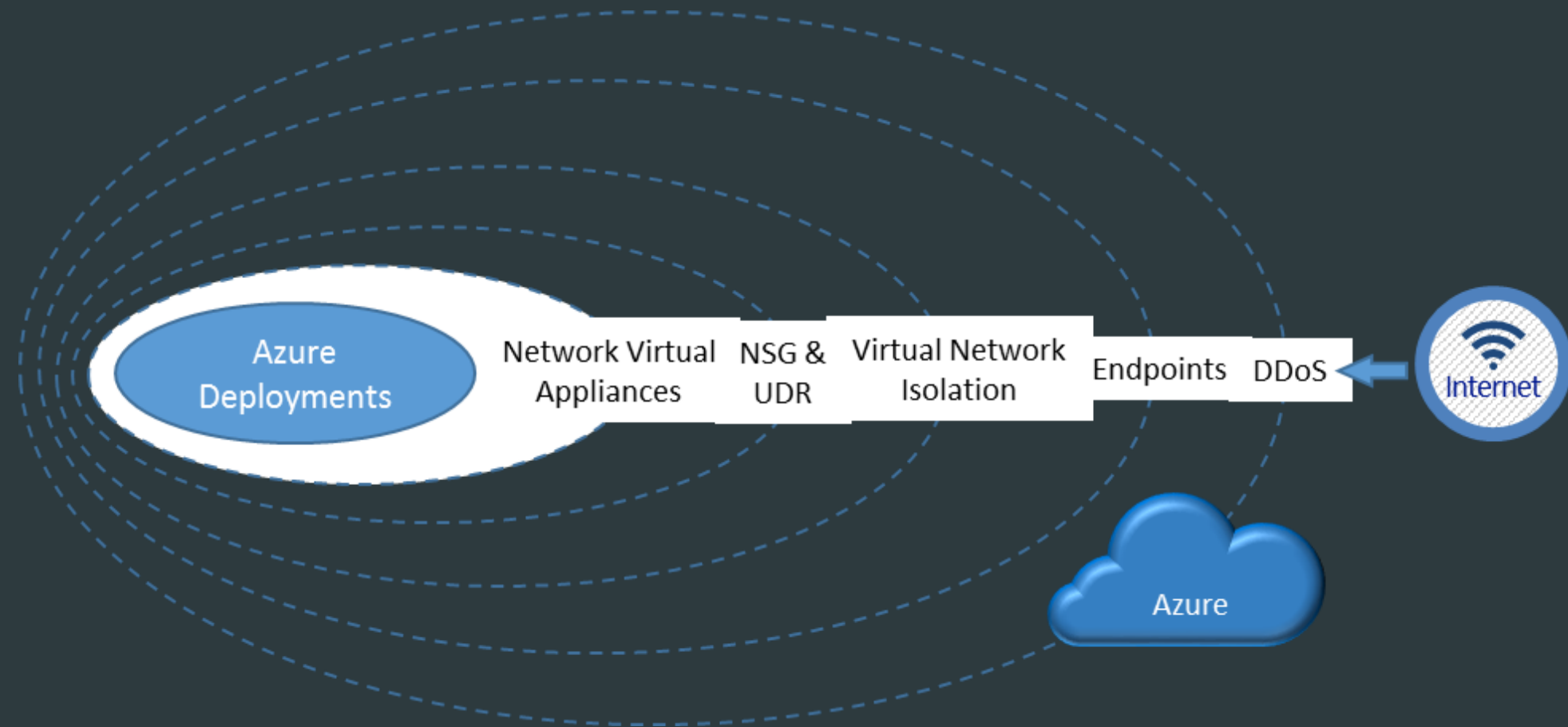
- NSG auf Subnetzebene zuerst ausgewertet, NSG auf NIC-Ebene als Nächstes

### Ausgehende Verbindungen

- NSG auf NIC-Ebene zuerst ausgewertet, NSG auf Subnetzebene als Nächstes



## Azure Netzwerk NSGs

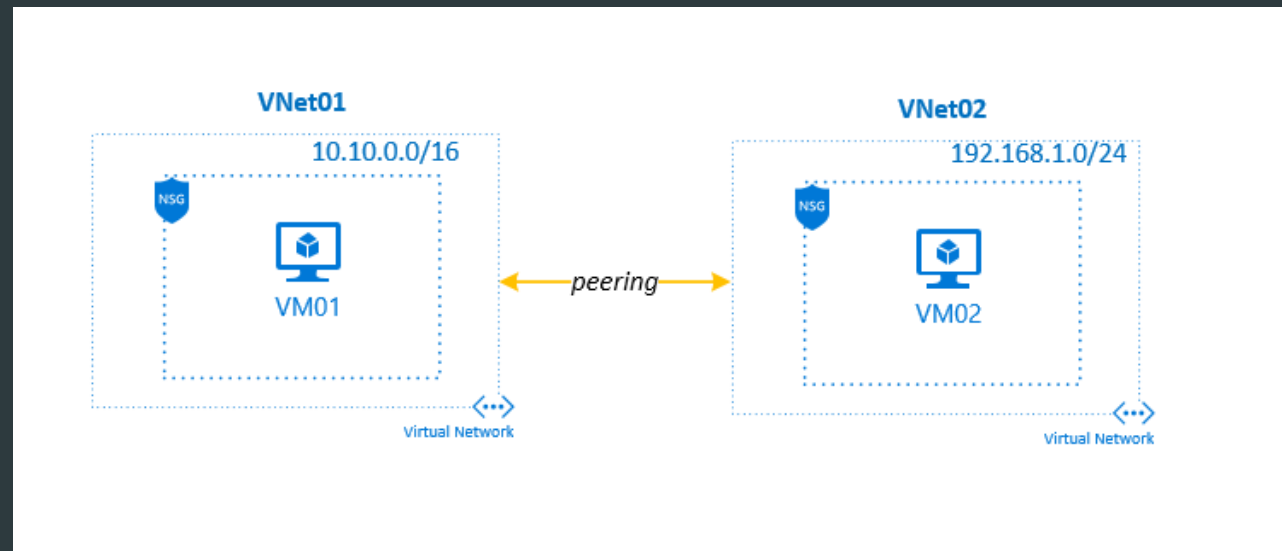




## Azure Netzwerk Peering

### Peering







- VNet Peering
  - VNets verbinden in der gleichen Region
- Global Vnet peering
  - Über regionale VNets verbinden
- Hohe Bandbreite
- Geringe Latenz
- Keine Verschlüsselung





## Azure Anbindung

# Microsoft Azure Hybrid Options

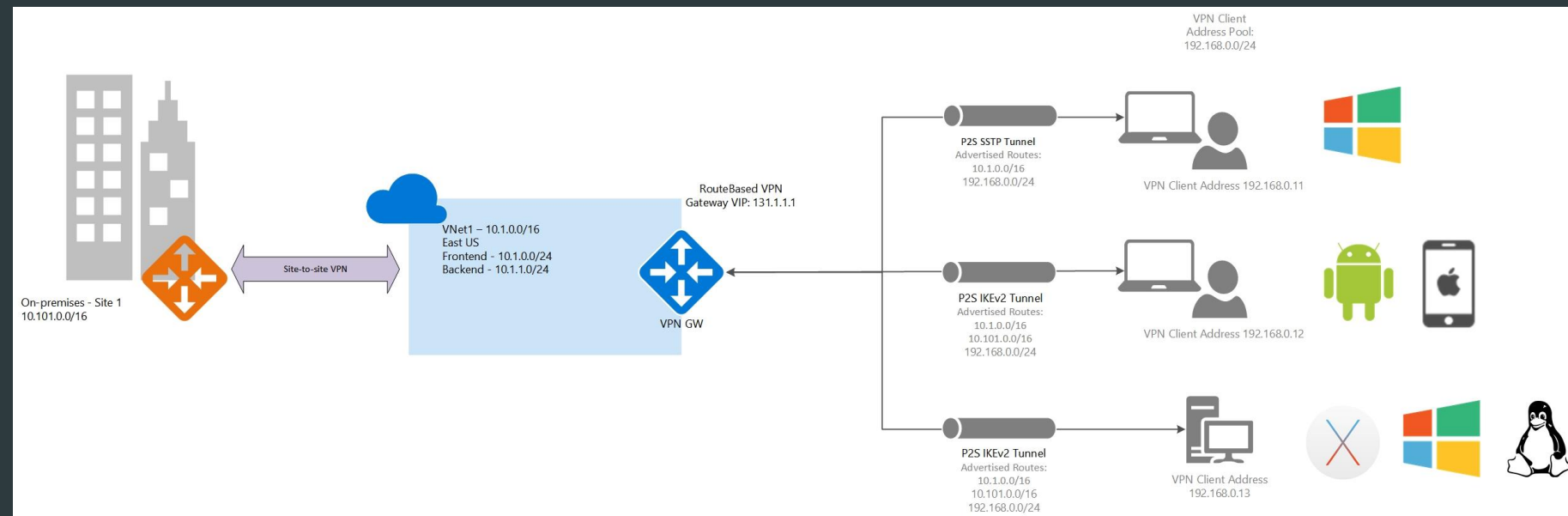
Cloud		Customer	Description
	Secure point-to-site connectivity Virtual Network (Point-to-Site)		<ul style="list-style-type: none"><li>• 80 Mbps</li><li>• Configure up to 254 clients to connect per virtual network.</li></ul>
	Secure site-to-site VPN connectivity Virtual Network (Site-to-Site)		<ul style="list-style-type: none"><li>• 80 Mbps</li><li>• Connect on-premises network to virtual network using IPSEC over the Internet</li></ul>
	Private site-to-site connectivity ExpressRoute		<ul style="list-style-type: none"><li>• 10 Mbps – 10 Gbps</li><li>• Direct connectivity through Exchange Provider or Network Service Provider to Azure.</li></ul>



## Azure Anbindung P2S

### P2S key facts

- Protokoll: SSL/TLS (TLS 1.2 only), SSTP, IKEv2
- Authentication: Zertifikate, Azure ADDS
- SSTP Connections: Max. 128
- IKEv2 Connections: zwischen 250 und 1000 (je nach Gateway Type)
- OS: Ab Win7, Mac OS X (ab Version 11), Linux, iOS,..

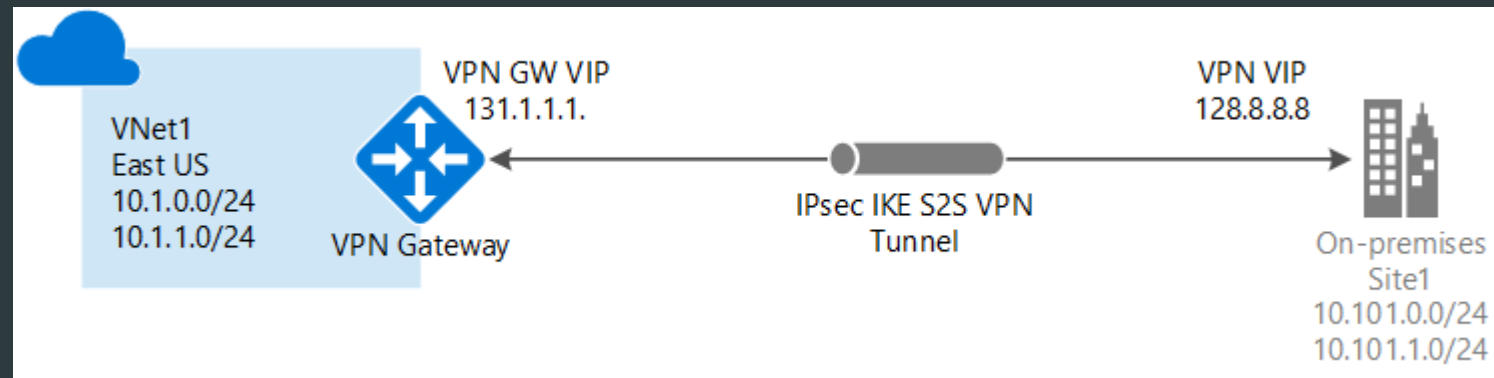




## Azure Anbindung S2S

### S2S key facts

- Protokoll: IPsec/IKE
- Connection resiliency: active-passive oder active-active
- SLA: von 99,9 – 99,95% je nach Gateway
- Bandbreite: 100 Mbps – 1,25 Gbps
- Site-to-Site oder Multi-Site connection



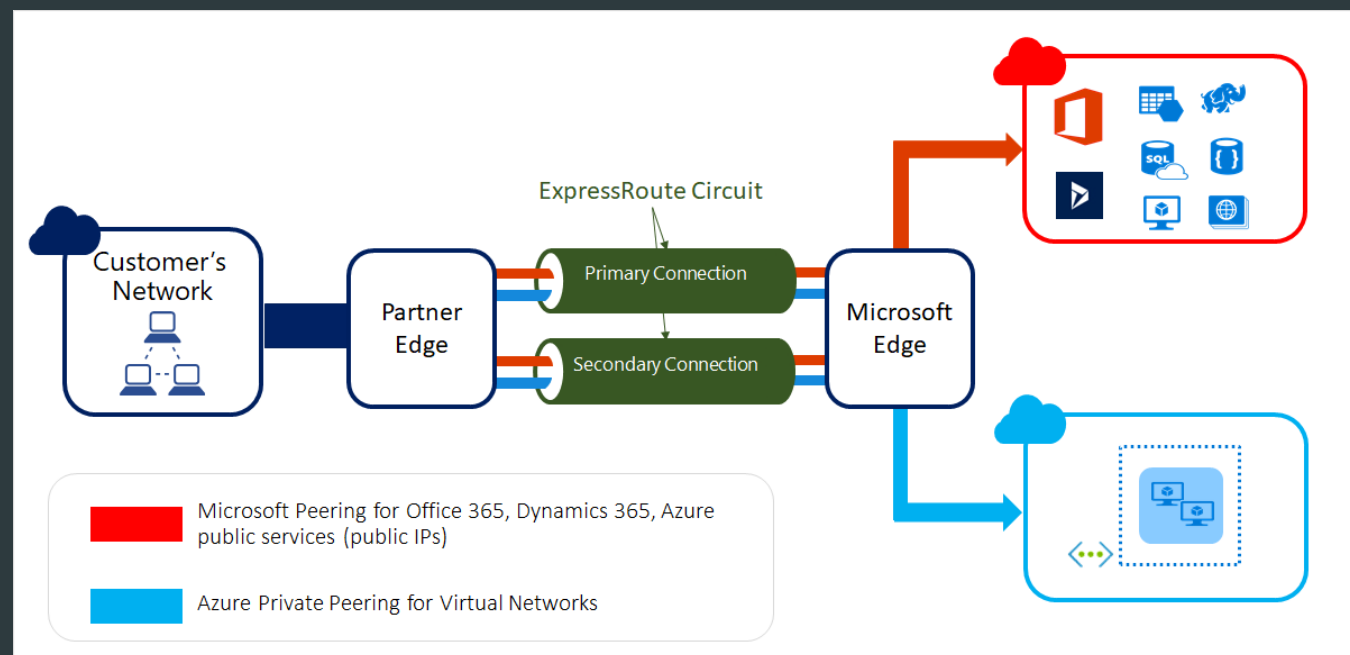




## Azure Anbindung ExpressRoute

### Express Route key facts

- Protokoll: Direkt Anbindung über VLANs, NSPs, VPN Technologie (MPLS, VPLS,...)
- Routing: BGP
- Connection resiliency: active-active
- SLA: von 99,9 – 99,95% je nach Gateway
- Bandbreite: 100 Mbps – 9 Gbps



# Demo

- Azure VNet
- Azure Subnetz
- Azure NSGs
- Azure Vnet Peering

# Kostenübersicht und Forecast- Möglichkeiten



## Azure Rechnung



















### Wie hoch wird die Rechnung am Ende des Monats sein?

- Azure Pricing calculator
  - Azure Hub Licensing
  - Azure reserved instances
- Azure Resource Cost/Resource Gruppe
- Azure Budget

# cost example

## Azure IaaS Sample



Load Balancer	 	Basic Load Balancer is free of charge	€0.00
Azure Backup	 	Azure VMs Type, 5 Instance(s) x 120 GB, LRS Redundanc...	€63.70
Application Gateway	 	Web Application Firewall tier, Medium Instance size: 1 G...	€124.86
Virtual Network	 	0 TB data transfer from West Europe region to West Eur...	€0.00
VPN Gateway	 	VPN Gateways type, Basic VPN tier, 744 gateway hour(s)...	€58.90
Traffic Manager	 	2 million DNS queries/mo, 1 Azure endpoint(s), 0 Fast A...	€1.67
Virtual Machines: AD	 	1 B2MS (2 vCPU(s), 8 GB RAM); Windows – (OS Only); 3 ...	€36.97
Virtual Machines: App + SQL Server	 	1 D2s v3 (2 vCPU(s), 8 GB RAM); Windows – (OS Only); 3...	€124.30
Virtual Machines: RDS	 	1 E4s v3 (4 vCPU(s), 32 GB RAM); Windows – (OS Only); ...	€222.63


Estimated monthly cost

€633.03

 Export

 Save

 Save as

 Share

Euro (€)

how to optimize costs?



**7am to 7pm  
workdays  
means min.  
61%  
Discount!!**

# Demo

- Azure Pricing Calculator
- Azure Resourcegroup Cost
- Azure Budget

# Recap dieses Workshops

- ✓ Was ist Azure?
- ✓ Wie kauft man Azure bzw. welche Vertragsarten gibt es?
- ✓ Ein Überblick über die Azure Services
- ✓ Sicherheit in der Azure Cloud
- ✓ Umgesetzte Use-Cases für die Cloud
- ✓ Netzwerk und Anbindungsmöglichkeiten an die Azure Cloud
- ✓ Kostenübersicht und Forecast-Möglichkeiten



# Feedback



## Hannes Lagler-Gruener

Cloud Solutions Architect, ACP  
P-CSA, Azure MCSE, AWS Cloud Practitioner

Blog <http://cloudblogger.at>

Sozial <https://www.linkedin.com/in/hannesl1>

## Feedback

- QR Code
- Azure Dashboard



# Vielen Dank

## Referenzen



Windows Azure – <https://azure.microsoft.com/en-in>

What is Windows Azure - [https://www.youtube.com/watch?v=poDRw\\_Xi3Aw](https://www.youtube.com/watch?v=poDRw_Xi3Aw)

Azure Demo - <https://www.youtube.com/watch?v=7V8HikBP1vQ>

Azure Blog - <https://azure.microsoft.com/en-in/blog/>

Blog Hannes Lagler-Gruener – <http://cloudblogger.at>